On some Representations of Quadratic APN Functions and Dimensional Dual Hyperovals (Algebraic Combinatorics and related groups and algebras)

AUTHOR(S):

Edel, Yves

CITATION:

Edel, Yves. On some Representations of Quadratic APN Functions and Dimensional Dual Hyperovals (Algebraic Combinatorics and related groups and algebras). 数理解析研究所講究録 2010, 1687: 118-130

ISSUE DATE:

2010-05

URL:

http://hdl.handle.net/2433/141484

数理解析研究所講究録
第1687巻 2010年 118-130

On some Representations of Quadratic APN Functions and Dimensional Dual Hyperovals

Yves Edel *
Department of Pure Mathematics and Computer Algebra
Ghent University, Krijgslaan 281, S22
B-9000 Ghent, Belgium

1. Introduction

APN functions (see Definition 1) have become a quite popular area of research and especially quadratic APN functions have links to various other mathematical areas. One link is to geometry, namely dimensional dual hyperovals (see Definition 2). Quadratic APN functions are equivalent to certain subspaces of the alternating bilinear forms, and most examples of dual hyperoval are, or can be, constructed from certain subspaces of the bilinear forms.

As consequence different related publications use substantially different notation. The present manuscript is based on the authors efforts to provide an explicit translation of the notation found in several papers on APN functions and dual hyperovals by Nakagawa, Taniguchi and Yoshiara, into his own notation and back.

The focus of this manuscript are the representations. An other important point, the question of equivalence is not touched. We refer to [14] for the characterization of the dual hyperovals that arise from quadratic APN functions via the construction as described in Proposition 6, for the correspondence of their mutual equivalence classes as well as for an explicit construction of the APN function, given an "APN-dual hyperoval".

Furthermore we restrict ourselves to the binary case, although some results hold also in more generality. Firstly as most results on APN functions are only for this case, secondly as the notation often gets substantially less complicated. For more extensive references, overviews over actual or more general results, open problems and motivations we refer to some recent overview articles [8, 9, 16, 22].

This manuscript is organized as follows: In the next section APN functions are introduced and several conditions for being quadratic are given. Section 3 deals with several ways of representing (alternating) bilinear forms as well as with representations of subspaces of this forms. Section 4 gives some characterizations of APN functions in terms of these subspaces. In Section 5 dimensional dual hyperovals will be introduced and characterized in terms of (alternating) bilinear forms. This section concludes with an alternative proof of Taniguchi's result [21, Theorem 11]. In the Appendix the trace representation of vector spaces of (alternating) bilinear forms will be discussed and the alternating subspaces, in this representation, coming from APN functions are treated in detail.

2. Quadratic APN functions

Definition 1. *Let $\mathbb{F}_p$ be the finite field with p elements, p prime. A function $f : \mathbb{F}_p^m \mapsto \mathbb{F}_p^n$ which satisfies*

$$\forall(a \in \mathbb{F}_p^m \setminus \{0\})\forall(b \in \mathbb{F}_p^n): \quad |\{x \in \mathbb{F}_p^m | f(x+a) - f(x) = b\}| \leq d$$

with $d = 1$, is called **perfect nonlinear (PN)** *or* **planar**. *The function f is called* **almost perfect nonlinear (APN)** *if it satisfies the equation with $d = 2$.*

PN functions do not exist in even characteristic. Due to the existence of PN functions in odd characteristic, APN functions are mostly only studied in characteristic 2 and the majority of papers on APN functions only deal with the (extremal) case $m = n$. However there exist also some results in an even more general setting, obtained by replacing the vector spaces in Definition 1 by arbitrary abelian groups (see e.g. [10, 18]).

A function $f : \mathbb{F}_p^m \to \mathbb{F}_p^n$ can be represented by n polynomials f_i in $\mathbb{F}_p[X_1, \ldots, X_m]$ (also called boolean functions, in the case $p = 2$). What is referred as **(algebraic) degree of an APN function** is maximum

*The research of this author takes place within the project "Linear codes and cryptography" of the Research Foundation – Flanders (FWO) (Project nr. G.0317.06), and is supported by the Interuniversitary Attraction Poles Programme - Belgian State - Belgian Science Policy: project P6/26-Bcrypt.

among the algebraic degrees $d^\circ(f_i)$ of the corresponding polynomials in m variables, i.e. the maximal number of variables, in a monomial with non vanishing coefficient, of the algebraic normal form of one of the f_i.

Quadratic APN functions are APN functions of degree 2. We will restrict us to quadratic APN functions.

If $n = m$ the same mapping considered as $f : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ can be represented as an univariate polynomial $f \in \mathbb{F}_{p^m}[X]$.

Let the p-weight of an integer be the sum of its coefficients in its p-adic representation, i.e:

$$w_p(\sum_{i=0}^{l} a_i p^i) := \sum_{i=0}^{l} a_i \in \mathbb{Z} \text{ with } 0 \leq a_i < p$$

The **p-weight of a univariate polynomial** is defined as

$$w_p(\sum_{i=0}^{l} u_i X^i) := \max\{w_p(i) |\ u_i \neq 0\}$$

The p-weight of the univariate polynomial equals the algebraic degree of the same map written as multivariate polynomial. This can be found e.g. in [9, Section 1.1], for $p = 2$, in more detail.

Univariate polynomials of p-weight 1 are called **linearized polynomials**, these are all $\mathbb{F}_p$-linear maps.

The (additive) **derivate** in (in direction $a \neq 0$) $D_a f$ is defined as

$$D_a f(x) = f(x + a) - f(x)$$

APN functions are defined by properties of their derivate (Definition 1). The derivate is not symmetric in x and a, we will define a symmetric version:

$$\delta_y f(x) := f(x + y) - f(x) - f(y) - f(0)$$

Direct verification shows that

$$\delta_{x_k} \ldots \delta_{x_2} f(x_1) = \sum_{I \subseteq \{1,\ldots,k\}} (-1)^{k-|I|} f(\sum_{i \in I} x_i).$$

For constant a the derivate $D_a(f)$ and $\delta_a f$ differ only by a constant. Substituting $D_a f$ by $\delta_a f$ in Definition 1 therefore will lead to equivalent definitions.

In the following we will always assume that $p = 2$.

Proposition 1. *The following characterization of a quadratic function are equivalent:*

- *f has algebraic degree $d^\circ(f) = 2$.*
- *For $n = m$: f has 2-weight $w_p(f) = 2$.*
- *For all $a \neq 0$ $D_a f$ is $\mathbb{F}_2$-linear ($\leftrightarrow$ additive $\leftrightarrow$ $d^\circ(D_a f) \leq 1$)*
- *$B_f(x, y) := \delta_y f(x) = f(x + y) + f(x) + f(y) + f(0)$ is an alternating bilinear function.*
- *$\delta_z \delta_y f(x) = f(x + y + z) + f(x + y) + f(y + z) + f(z + x) + f(x) + f(y) + f(z) + f(0)$ is constant zero.*

Proof. The argumentation relays on the (unproven) property that for a non-constant function f, the algebraic degree of $\delta_y f(x)$, viewed as function in x, is smaller than the algebraic degree of f and is (exactly) $d^\circ f - 1$, if $d^\circ f > 1$. The verification of this remark is straight forward but lengthly and therefore omitted.

Direct verification shows that $B_f(x, y)$ is symmetric and $B_f(x, x) = 0$.

Assume f is quadratic. The above remark states that $B_f(x, y)$ is linear as function in x. By symmetry it is bilinear. $\delta_z \delta_y f(x)$ is a constant (as derivate of a linear function). Choose $x = y = z = 0$. This show that this constant is zero.

Now assume that the algebraic degree of f is larger than 2. By the remark we have that $B_f(x, y)$ is not linear in x and $\delta_z \delta_y f(x)$ not constant. □

3. On the vector space of (alternating) bilinear forms

3.1. Bilinear forms

We now look on different (unique) representations for a bilinear form. A **bilinear form** is a map

$$b(x,y) : \mathbb{F}_2^l \times \mathbb{F}_2^m \mapsto \mathbb{F}_2 \text{ for which } b(x+x',y) = b(x,y) + b(x',y) \text{ and } b(x,y+y') = b(x,y) + b(x,y').$$

In case $l = m$, a bilinear form $b(x,y)$ is called **alternating** if additionally, for all $x \in \mathbb{F}_2^m$, $b(x,x) = 0$ (this implies that $b(x,y) = b(y,x)$).

Choose some basis $e_1, \ldots, e_u$ of $\mathbb{F}_2^u$ and write an $x \in \mathbb{F}_2^u$ as $x = \sum_{i=1}^{u} x_i e_i$, $x_i \in \mathbb{F}_2$.

3.1.1. The matrix representation.

The perhaps most basic representation of a bilinear form is by a matrix $M \in \mathbb{F}_2^l \times \mathbb{F}_2^m$.

$$b(x,y) = x^t M y = \sum_{i=1}^{l}\sum_{j=1}^{m} x_i m_{i,j} y_j, \text{ where } m_{i,j} = b(e_i, e_j) \in \mathbb{F}_2 \tag{1}$$

An alternating form ($l = m$) is given by a symmetric matrix ($m_{i,j} = m_{j,i}$) with main diagonal zero ($m_{i,i} = 0$).

3.1.2. Representation using the tensor product, Variant 1

Identify the $(x,y) \in \mathbb{F}_2^l \times \mathbb{F}_2^m$, with the tensor product $(x \otimes y) := \sum_{i,j} x_i y_j (e_i \otimes e_j) \in \mathbb{F}_2^l \otimes \mathbb{F}_2^m$. Any bilinear form can be uniquely written using a linear map $\gamma : \mathbb{F}_2^n \otimes \mathbb{F}_2^n \to \mathbb{F}_2$ (this is the so called universal property of the tensor product).

$$b(x,y) = (x \otimes y)^\gamma = \sum_{i,j} x_i y_j (e_i \otimes e_j)^\gamma = \sum_{i,j} x_i y_j m_{i,j}, \text{ where } m_{i,j} = (e_i \otimes e_j)^\gamma = b(e_i, e_j) \in \mathbb{F}_2$$

By the same reasoning an alternating bilinear form can be given through a linear map $\gamma : \mathbb{F}_2^m \wedge \mathbb{F}_2^m \to \mathbb{F}_2$. The vector space $\mathbb{F}_2^m \wedge \mathbb{F}_2^m$ can be viewed as the subspace of $\mathbb{F}_2^m \otimes \mathbb{F}_2^m$ generated by the elements $(e_i \otimes e_j) + (e_j \otimes e_i) =: (e_i \wedge e_j)$. Observe $(x \wedge y) = 0$ and $(x \wedge y) = (y \wedge x)$. We get:

$$b(x,y) = (x \wedge y)^\gamma = \sum_{i<j} (x_i y_j + x_j y_i)(e_i \wedge e_j)^\gamma = \sum_{i,j} (x_i y_j + x_j y_i) m_{i,j}, \text{ where } m_{i,j} = (e_i \wedge e_j)^\gamma = b(e_i, e_j) \in \mathbb{F}_2$$

3.1.3. Representation using the tensor product, Variant 2

Observing that the vector space of all bilinear form $\mathbb{F}_2^l \times \mathbb{F}_2^m \to \mathbb{F}_2$ has the same dimension over $\mathbb{F}_2$ as $\mathbb{F}_2^l \otimes \mathbb{F}_2^m$, a bilinear form can be identified with an element (or equivalently a 1-dimensional subspace) of $\mathbb{F}_2^l \otimes \mathbb{F}_2^m$ by fixing a vector space isomorphism. We will use:

$$\sum_{i,j} u_{i,j} (e_i \otimes e_j) \leftrightarrow b(x,y) = \sum_{i,j} x_i y_j u_{i,j}.$$

Proceeding analogously for alternating bilinear forms gives:

$$\sum_{i<j} u_{i,j} (e_i \wedge e_j) \leftrightarrow b(x,y) = \sum_{i<j} (x_i y_j + x_j y_i) u_{i,j}.$$

Then there is a nice correspondence between Variant 1 and Variant 2. An element $\sum_{i,j} u_{i,j}(e_i \otimes e_j)$ corresponds to the map $\gamma : (e_i \otimes e_j) \mapsto u_{i,j}$. And every linear map $\gamma : \mathbb{F}_2^l \otimes \mathbb{F}_2^m \to \mathbb{F}_2$ defines the element $\sum_{i,j} (e_i \otimes e_j)^\gamma (e_i \otimes e_j)$. The same bilinear form is obtained if we apply the image under this corespondents in the respective variant.

For alternating bilinear forms we proceed analogously.

3.1.4. Representation as polynomial in x_i, y_i.

Any function $b(x,y) : \mathbb{F}_2^l \times \mathbb{F}_2^m \mapsto \mathbb{F}_2$ can be written as polynomial in $F_2[x_1, \ldots, x_l, y_1, \ldots, y_m]$. The function is bilinear, if its algebraic degree with respect to the variables $x_1, \ldots, x_l$, as well as with respect to the variables $y_1, \ldots, y_m$ is one. I.e. (again) we have that

$$b(x,y) = \sum_{i,j} m_{i,j} x_i y_j, \text{ where } m_{i,j} = b(e_i, e_j) \in \mathbb{F}_2$$

$b(x,y)$ is an alternating form if $m_{i,j} = m_{j,i}$ and $m_{i,i} = 0$. This is just the matrix representation under a different point of view.

3.1.5. The trace representation

Let $l = m$. Consider x, y now as elements of the field $\mathbb{F}_{2^m}$. The $(\mathbb{F}_2)$-bilinear form $b(x,y) : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \mapsto \mathbb{F}_2$ can be uniquely given in the form

$$b(x,y) = \mathrm{tr}(l(x)y) \text{ with } l(x) = \sum_{k=0}^{m-1} \alpha_k x^{2^k} \tag{2}$$

This representation is usually dedicated to Delsarte and Goethals [12]. It will be refered in the following as the **trace representation** of a bilinear form.

We also identify $b(x,y)$ with the element $(\alpha_0, \ldots, \alpha_{m-1}) \in (\mathbb{F}_{2^m})^m$ which defines the linearized polynomial l.

For alternating bilinear forms, the same representation as in Equation 2 is obtained, only the linearized polynomial l is of special form:

$$\alpha_0 = 0, \quad \alpha_k = \alpha_{m-k}^{2^k}, \quad \text{Especially if } m = 2r: \ \alpha_r = \alpha_r^{2^r}, \text{ i.e. } \alpha_r \in \mathbb{F}_{2^r}$$

So the trace representation of an alternating form is determined by the element

$$(\alpha_1, \ldots \alpha_r) \in \begin{cases} (\mathbb{F}_{2^m})^{r-1} \times \mathbb{F}_{2^r} & \text{if } m = 2r \\ (\mathbb{F}_{2^m})^r & \text{if } m = 2r+1 \end{cases}$$

Details on the trace representation, and explicit conversions to the other representations have been transferred to the Appendix A, as they need some room.

3.2. Vector spaces of bilinear forms

3.2.1. Basic definitions

The bilinear forms $b(x,y) : \mathbb{F}_2^l \times \mathbb{F}_2^m \to \mathbb{F}_2$ form a lm-dimensional vector space which will be denoted as $\mathcal{B}(x,y)$. Define a scalar product:

$$\langle , \rangle : \mathcal{B}(x,y) \times \mathcal{B}(x,y) \to \mathbb{F}_2, \quad \langle \sum_{i,j} m_{i,j} x_i y_j, \sum_{i,j} m'_{i,j} x_i y_j \rangle := \sum_{i,j} m_{i,j} m'_{i,j}$$

The alternating bilinear forms $b(x,y) : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2$ form a $\binom{m}{2}$-dimensional vector space which will be denoted as $\mathcal{A}(x,y)$. We define a scalar product on $\mathcal{A}(x,y)$:

$$\langle , \rangle_a : \mathcal{A}(x,y) \times \mathcal{A}(x,y) \to \mathbb{F}_2, \quad \langle \sum_{i<j} m_{i,j}(x_i y_j, + x_j y_i), \sum_{i<j} m'_{i,j}(x_i y_j, + x_j y_i) \rangle_a := \sum_{i<j} m_{i,j} m'_{i,j}$$

Observe $\langle , \rangle_a$ is not the restriction of $\langle , \rangle$ on $\mathcal{A}$ viewed as subspace of $\mathcal{B}$. An adapted scalar product for the trace representation is defined in Appendix A.

For a subspace $B(x,y) \subseteq \mathcal{B}(x,y)$ (resp $B(x,y) \subseteq \mathcal{A}(x,y)$) define the **dual subspace** $B^\perp(x,y)$ as

$$\begin{aligned} B^\perp(x,y) &:= \{b'(x,y) \in \mathcal{B}(x,y) | \forall b \in B : \langle b'(x,y), b(x,y) \rangle = 0\} \subseteq \mathcal{B} \\ B^\perp(x,y) &:= \{b'(x,y) \in \mathcal{A}(x,y) | \forall b \in B : \langle b'(x,y), b(x,y) \rangle_a = 0\} \subseteq \mathcal{A} \end{aligned}$$

Dual subspaces in the trace representation are teated in Appendix A.2.

The **left radical** $\mathsf{lR}(b)$, $b \in \mathcal{B}(x,y)$ (resp. $\mathcal{A}(x,y)$), is the subspace

$$\mathsf{lR}(b) := \{x \in \mathbb{F}_2^l | \forall y \in \mathbb{F}_2^m : (b(x,y) = 0)\} \subseteq \mathbb{F}_2^l.$$

The **right radical** rR is defined analogously. The **rank** $\mathsf{rank}(b)$ of $b(x,y) \in \mathcal{B}(x,y)$ (resp. $\mathcal{A}(x,y)$) is defined as the codimension of the left radical. The rank of $b(x,y) = \sum_{i,j} m_{i,j} x_i y_j$ equals the rank of the matrix $(m_{i,j})$. Hence the rank of $b(x,y)$ also equals the codimension of the right radical.

A well known property of alternating forms is that every $b \in \mathcal{A}(x,y)$ has even rank.

The straight forward method of giving a n-dimensional subspace of $\mathcal{B}(x,y)$ (resp $\mathcal{A}(x,y)$), for any chosen representation of bilinear forms, is to give a basis b_i or a generator set of the subspace (or its dual).

By choosing a basis f_i of $\mathbb{F}_2^n$ (or of any n-dimensional subspace V) the subspace B can be associated with the bilinear map

$$B(x,y) : \mathbb{F}_2^l \times \mathbb{F}_2^m \to \mathbb{F}_2^n, \quad B(x,y) := \sum_{i=1}^{n} f_i b_i(x,y) \tag{3}$$

Reversing the process gives us, from a bilinear map $B(x,y) : \mathbb{F}_2^l \times \mathbb{F}_2^m \to \mathbb{F}_2^n$, a n-dimensional subspace of $\mathcal{B}(x,y)$ (resp $\mathcal{A}(x,y)$).

In the special case $l = m$, the alternating bilinear map $B_f(x,y) : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2^n$ can be represented by a quadratic function f (see Proposition 1). From [14, Lemma 4,5] follows that f can be reconstructed, up to equivalence, from B_f and that equivalent alternating bilinear forms $B_f, B_{f'}$ lead to EA-equivalent quadratic functions f and f' and vice versa (the APN condition is not used in the proof).

A geometric characterization quadratic APN functions f (and hence also of the corresponding alternating bilinear form B_f) will be given in Proposition 6. More details are to be found in [14].

In the case that $l = m$, the n-dimensional subspace of $\mathcal{B}$, resp. $\mathcal{A}$ can also be represented in terms of the trace representation. If $l = m = n$ the subspace can be given by an $\mathbb{F}_2$-linear or linearized polynomial in two variables $\mathbb{F}_{2^m}[X,Y]$. This will be done in Appendix A.

3.2.2. On representations of subspaces of bilinear forms using the tensor notation

If we use the tensor notation for bilinear forms as introduced in Sections 3.1.2 and 3.1.3, we have two further possibilities.

Variant 2: This is based on Variant 2 for the forms (see Section 3.1.3). There, a bilinear form $b \in \mathcal{B}$ (resp. $\mathcal{A}$) was identified with an element of $\mathbb{F}_2^l \otimes \mathbb{F}_2^m$ (resp $\mathbb{F}_2^m \wedge \mathbb{F}_2^m$), hence a subspace $B \subseteq \mathcal{B}$ (resp. $\mathcal{A}$) will simply be identified with a subspace S of $\mathbb{F}_2^l \otimes \mathbb{F}_2^m$ (resp $\mathbb{F}_2^m \wedge \mathbb{F}_2^m$). Explicitly:

$$\begin{aligned} B(x,y) &:= \{b(x,y) = \sum_{i,j} m_{i,j} x_i y_j | \sum_{i,j} m_{i,j}(e_i \otimes e_j) \in S\} \subseteq \mathcal{B} \\ B(x,y) &:= \{b(x,y) = \sum_{i<j} m_{i,j}(x_i y_j + x_j y_i) | \sum_{i<j} m_{i,j}(e_i \wedge e_j) \in S\} \subseteq \mathcal{A} \end{aligned}$$

Observe that $S^\perp$ (with respect to the standard scalar product) gives us this way $B^\perp(x,y)$.

Variant 1: This is based on Variant 1 for the forms (see Section 3.1.2). Let V be a n-dimensional subspace over $\mathbb{F}_2$ and Γ a surjective linear map $\Gamma : \mathbb{F}_2^l \otimes \mathbb{F}_2^m \mapsto V$ (resp. $\Gamma : \mathbb{F}_2^m \wedge \mathbb{F}_2^m \mapsto V$). The map Γ can be used to give an (alternating) bilinear map $\beta : \mathbb{F}_2^l \times \mathbb{F}_2^m \mapsto V$ (resp. $\beta : \mathbb{F}_2^l \wedge \mathbb{F}_2^m \mapsto V$), which can be defined analog to Section 3.1.2 as

$$\beta(x,y) = (x \otimes y)^\Gamma = \sum_{i,j} x_i, y_j (e_i \otimes e_j)^\Gamma \quad (\text{resp. } (x \wedge y)^\Gamma = \sum_{i,j} (x_i y_j + x_j y_i)(e_i \wedge e_j)^\Gamma)$$

This, essentially, already gives us a n-dimensional subspace B of (alternating) bilinear forms and of $\mathbb{F}_2^l \otimes \mathbb{F}_2^m$ (resp. $\mathbb{F}_2^m \wedge \mathbb{F}_2^m$), but let's do it explicitly.

Choose a basis $f_1, \ldots, f_n$ of V over $\mathbb{F}_2$, then $\Gamma = \sum_i f_i \gamma_i$ for some $\gamma_i : \mathbb{F}_2^l \otimes \mathbb{F}_2^m \mapsto \mathbb{F}_2$ (resp. $\gamma_i : \mathbb{F}_2^m \wedge \mathbb{F}_2^m \mapsto \mathbb{F}_2$). It is equivalent:

- Γ is a surjective map.
- The projection of Γ on any 1-dimensional subspace of V is non-trivial.
- V and the space spanned by the γ_i have equal dimension.

Identify the linear maps γ_i with the elements $\tilde{\gamma}_i \in \mathbb{F}_2^l \otimes \mathbb{F}_2^m$ (as in Section 3.1.3). The $\tilde{\gamma}_i$ span a n-dimensional subspace $\tilde{\Gamma}$ of $\mathbb{F}_2^l \otimes \mathbb{F}_2^m$ (resp. $\mathbb{F}_2^m \wedge \mathbb{F}_2^m$). Using "Variant 2" gives us now a vector space of bilinear forms.

It will turn out useful for Corollary 4 to observe that for $\ker(\Gamma)$, the kernel of Γ, we have

Proposition 2.

$$\ker(\Gamma) = \tilde{\Gamma}^\perp$$

Proof. As observed in Section 3.1.3 we have that

$$\tilde{\gamma}_k = \sum_{i,j} (e_i \otimes e_j)^{\gamma_k} (e_i \otimes e_j)$$

Hence for any $\sum_{i,j} u_{i,j}(e_i \otimes e_j) \in \tilde{\Gamma}^\perp$ and for all $1 \le k \le n$,

$$0 = \langle \sum_{i,j} u_{i,j}(e_i \otimes e_j), \tilde{\gamma}_k \rangle = \sum_{i,j} u_{i,j}(e_i \otimes e_j)^{\gamma_k} = (\sum_{i,j} u_{i,j}(e_i \otimes e_j))^{\gamma_k}$$

by definition of duality. Hence $\Gamma^\perp$ is in the kernel of each γ_k, and so also in the kernel of $\Gamma = \sum_i f_i\gamma_i$.
If Γ is surjective, then the dimension of V is the codimension of $\Gamma^\perp$, hence $\Gamma^\perp$ is the full Kernel.

For the alternating case we have the analog proof. □

As a subspace is unequally determined by its dual this implies that the subspace of bilinear forms given by Γ is uniquely determined by the kernel of the map Γ. This characterization via the kernel of Γ is e.g. found in [20,22].

4. Different characterizations of APN functions

For a quadratic APN function f the derivate

$$B_f(x,y) = \delta_y f(x) = f(x+y) + f(x) + f(y) + f(0)$$

is an alternating bilinear function $B(x,y) : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^n}$. Let the alternating bilinear function given by a linear function Γ, so $B(x,a) = (x \wedge a)^\Gamma$ (see Section 3.2.2, Variant 1).

A (quadratic) function f is APN if and only if for all $a \neq 0$ the only nonzero solution x of $B(x,a)$ is $x = a$. Observe $(0 \wedge a) = (a \wedge a) = 0 \in \mathcal{A}$ and $0 \neq (x \wedge a) \in \mathcal{A}$ for $x \neq 0, a$.
As $B(x,a) = (x \wedge a)^\Gamma$, we have that f is APN if and only if no vector of the form $x \wedge a$, $x \neq 0, a$, is in the kernel of Γ.

Following Nakagawa [20] call an element $x \wedge y$, $0 \neq x \neq y \neq 0$, a **pure element** of $\mathcal{A}$. This leads to the following characterization of APN functions:

Proposition 3. *f is APN if and only if the kernel of Γ contains no pure element ($\leftrightarrow$ no pure 1-dim subspace).*

It will be useful to have some more notation for subsets of $\mathcal{A}$, introduced by Delsarte and Goethals [12], and for subsets of $\mathcal{B}$ introduced by Delsarte in [11]. We specialize the definitions, which were given in [11,12] for subsets of $\mathcal{A}$ resp. $\mathcal{B}$, here to subspaces and mostly focus on $\mathcal{A}$.

In [11] the **q-distance** $d(b,b') := \mathsf{rank}(b - b')$ for elements in $b, b' \in \mathcal{B}$ is introduced. Also define the **q-weight** $w(b) := \mathsf{rank}(b)$. (Perhaps we should call it here the 2-weight and 2-distance).
A subspace $B \in \mathcal{B}$ is called a **t-design** if all nonzero elements of $B^\perp$ have q-weight greater then t [11]. As Delsarte himself stresses the analogy with error correction codes it would be natural to name $B^\perp$ a code in $\mathcal{B}$ of minimal distance $t+1$.
A subspace of alternating bilinear forms $\mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2$, $B \in \mathcal{A}$ is called in [12] a **(m,d)-set** if all nonzero elements of B have q-weight at least $2d$ (so if it is a "code" of minimal distance $2d$).
The cardinality of a (m,d)-set B is bounded by

$$|B| \leq 2^{\binom{m}{2}\frac{(r-d+1)}{r}} \qquad \text{with } r = \lfloor \frac{m}{2} \rfloor$$

A (m,d)-set obtaining this bound is called **maximal** [12].
For subspaces of $\mathcal{B}$ and $\mathcal{A}$ the **weight distribution** $(a_0, \ldots a_m)$ of $B \in \mathcal{B}$ (resp $(a_0, \ldots a_r)$ of $B \in \mathcal{A}$) is defined by $a_i = |\{b \in B | \, wt(b) = i\}|$, (resp. by $a_i = |\{b \in B | \, wt(b) = 2i\}|$).
For subspaces, the weight distribution of $B^\perp$ is uniquely determined by the weight distribution of B and can be computed with a "MacWilliams-like" transformation.
The weight distribution of maximal (m,d)-sets is uniquely determined [12, Theorem 4.ii], and for subspaces the dual of a maximal (m,d)-set is a (maximal) $(m, r-d+2)$-set [12, Theorem 5]. An OA-like characterization of a t-design in $\mathcal{A}$ (i.e. of the "dual code") is given by Munemasa [19, Theorem 1]
Analog results for subsets of $\mathcal{B}$ can be found in [11].

Next we want to give the APN condition in the case that B is given in terms of subspaces of $\mathcal{A}$ (see Section 3.2.2, Variant 2).

Proposition 4. *f is APN if and only if $B^\perp \subseteq \mathcal{A}$ is a $(m,2)$-set ($\leftrightarrow$ $B^\perp$ is a "code" of distance 4).*

Proof. We start from Proposition 3 and use Proposition 2. That $\ker(\Gamma) = B^\perp$ is a $(m,2)$-set is equivalent to: that for all non-zero $b \in B^\perp$ the $\mathsf{rank}(b) \geq 4$, i.e. (as bilinear forms of $\mathcal{A}$ have even rank) that there is no b with $\mathsf{rank}(b) = 2$. Hence it only remains to show that for an alternating bilinear form b it is equivalent:

- $b(x,y)$ hat rang 2
- $b(x,y)$ corresponds to a pure element of $\mathbb{F}_2^m \wedge \mathbb{F}_2^m$.

This follows by Proposition 5 below. □

Proposition 5. *The elements of rank $2r$ in $\mathcal{A}$ are the elements $\sum_{i=1}^{r}(x_i \wedge y_i)$ with some $x_1, \ldots, x_r, y_1, \ldots, y_r \in \mathbb{F}_2^m$ which are linearly independent.*

Proof. The generic alternating bilinear form of rank $2r$ is $B(x,y) = \sum_{i=1}^{r} x_{2i-1}y_{2i} + x_{2i}y_{2i-1}$ which corresponds to the element $\sum_{i=1}^{r}(e_{2i-1} \wedge e_{2i}) \in \mathcal{A}$.

Any other alternating bilinear form of rank $2r$ can be obtained by a base change i.e. by the substitution $x' = Lx$, $y = Ly$, with L a $m \times m$ matrix of full rank. Hence $B'(x,y) = B(x',y') = B(Lx, Ly)$. The corresponding element in $\mathcal{A}$ is $\sum_{i=1}^{r}(Le_{2i-1} \wedge Le_{2i})$.

As L is nonsingular, we have that the $2r$ elements $Le_i \in \mathbb{F}_2^m$ are arbitrary linear independent elements. □

Observe that for odd m, if $m = n$, the $(m,2)$-set $B^{\perp}$ in Proposition 4 is maximal, with [12, Theorem 5] we get

Corollary 1. *Let $m = 2r+1$. Then $f : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is APN if and only if $B \in \mathcal{A}$ is a (m,r)-set, or equivalently, if and only if all $0 \neq b \in B$ have rank $n-1$.*

5. Dual Hyperovals

Definition 2. *A set $\mathcal{V}$ of $d+1$-dimensional subspaces in a vector space over $\mathbb{F}_2$ is called a* **(d−dimensional) dual hyperoval** *if*

H1 *For any $V \neq V' \in \mathcal{V}$, $V \cap V'$ is 1-dimensional.*

H2 *Any three mutually different $V_i \in \mathcal{V}$ intersect in zero.*

H3 $|\mathcal{V}| = 2^{d+1}$.

The space spanned by the subspaces of $\mathcal{V}$ is called the **ambient space**.

There is a construction of $(m-1)$-dimensional dual hyperovals with help of a bilinear map $B : \mathbb{F}_2^m \times \mathbb{F}_2^m \mapsto \mathbb{F}_2^n$ due to Yoshiara [23] (see also [18]). Define:

$$\mathcal{V}_B := \{V_a \mid a \in \mathbb{F}_2^m\}, \quad V_a := \{(x, B(x,a)) \mid x \in \mathbb{F}_2^m\} \tag{4}$$

The ambient space is $\mathbb{F}_2^{n+m}$ (if B is surjective). $\mathcal{V}_B$ fulfills condition **H3** by construction.

Let $B_f(x,y) = \delta_y f(x) = f(x+y) + f(x) + f(y) + f(0) \subseteq \mathcal{A}$. We have the following characterization of quadratic APN functions (straight forward, see e.g. [14, 18, 23])

Proposition 6. *$f : \mathbb{F}_2^m \times \mathbb{F}_2^m \mapsto \mathbb{F}_2^n$ is a quadratic APN function if an only if $\mathcal{V}_{B_f}$ is a dual hyperoval.*

For $\mathcal{V}_B$ therefore it is handy to give conditions **B1** and **B2**, in terms of the bilinear map B, which are equivalent to the defining conditions **H1** and **H2** of a dual hyperoval. Let:

B1 For any $y \neq 0$ the map $M_y : x \mapsto B_{\mathcal{V}}(x,y)$ has rank $m-1$.

B2 The map $\sigma : y \mapsto kernel(M_y)$ is an bijection on $\mathbb{F}_2^m \setminus \{0\}$.

We have the following equivalences: $V_a \cap V_b \leftrightarrow B(x,a) = B(x,b) \leftrightarrow x \in \ker M_{a+b}$. **H1** says that for all $a \neq b$ this kernel has to be 1-dimensional, which is equivalent to **B1**.

Observe that a, b, c are mutually different if and only if $a+b, b+c, c+a$ are mutually different and nonzero.

H2 says that for any mutually different a, b, c the kernels $\ker M_{a+b}$, $\ker M_{b+c}$ and $\ker M_{c+a}$ hence $\sigma(a+b)$, $\sigma(b+c)$ and $\sigma(c+a)$ have to be different. It follows that $\sigma : \mathbb{F}_2^m \setminus \{0\} \to \mathbb{F}_2^m \setminus \{0\}$ has to be injective. As image and preimage are finite and of equal size, this is equivalent to **B2**, so **H2** → **B2**. On the other hand, if σ is bijective we have that for mutually different a, b, c also $\sigma(a+b)$, $\sigma(b+c)$ and $\sigma(c+a)$ are mutually different. $\sigma(a+b)$ determines the intersection point of V_a and V_b, so **B2** → **H2**.

Next we give an alternative condition for **B2** which is of the form of **B1**.

Lemma 2. *Let M_y and σ be defined as above. Assume* **B1** *holds, hence that for $y \neq 0$ the kernel $\ker(M_y)$ is 1-dimensional. Then the following statements are equivalent:*

1. **B2**
2. **B3**: *For any $x \neq 0$ the map $N_x : y \mapsto B(x,y)$ has rank $m-1$.*

Proof. By assumption it is $B(\sigma(y), y) = 0$.
$1 \Rightarrow 2$: Assume that σ is a permutation. Then, for fixed $x \neq 0$, there is exactly one y (i.e. $y = \sigma^{-1}(x)$) such that $B(x, y) = 0$. So $\sigma^{-1}(x)$ is the only non-zero element in $\ker(N_x)$.
$2 \Rightarrow 1$: Assume that for $x \neq 0$ the kernel $\ker(N_x)$ is 1-dimensional. Assume σ is no permutation. Then there is an element $v \neq 0$ which is not an image of σ. Hence $B(v, y) \neq 0$ for all $y \neq 0$, so $\ker(N_v) = 0$, a contradiction to the assumption. □

For subspaces $V \subseteq \mathbb{F}_2^u$ the **dual subspace** $V^\perp$ is defined as $V^\perp = \{v' \in \mathbb{F}_2^u | \forall v \in V : \langle v, v' \rangle = 0\}$. The **dual** $\mathcal{V}^\perp$of a dual hyperoval $\mathcal{V}$ is defined as $\mathcal{V}^\perp = \{V | V^\perp \in \mathcal{V}\}$.

We now introduce some bilinear forms associated to the bilinear form B. For one, as these bilinear forms are sources of new dual hyperovals. For two, as we then can characterize dual hyperovals entirely "natural" properties of bilinear forms, i.e. get rid of the linear maps M_y and N_x.

Definition 3. *Let B be an n-dimensional vector space of bilinear forms $B : \mathbb{F}_2^l \times \mathbb{F}_2^m \to \mathbb{F}_2$ and $\psi : B \to \mathbb{F}_2^n$ a vector space isomorphism. Define the l-dimensional vector space of bilinear forms $B^\dagger : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{F}_2$ as*

$$B^\dagger := \{b_x^\dagger | x \in \mathbb{F}_2^l\}, \quad b_x^\dagger(z, y) = \psi^{-1}(z)(x, y)$$

Different isomorphisms ψ lead to isomorphic vector spaces of bilinear forms $B^\dagger$. Define also:

$$B^*(y, x) = B(x, y)$$

Notation will get considerably more comfortable if we choose the right bases and always identify a vector space of bilinear forms with a bilinear map to a vector space of the same dimension.

Choose a basis e_i of $\mathbb{F}_2^l$, and a basis f_i of $\mathbb{F}_2^n$. Denote their dual bases (with respect to the standard scalar product) as $\bar{e}_i$, resp. $\bar{f}_i$. Choose as well a basis b_i of B.
Identify B with the map $B(x, y) = \sum_i \bar{f}_i b_i(x, y)$. Choose ψ as the map $b_i \mapsto f_i$. Then:

$$b_x^\dagger(z, y) = \psi^{-1}(z)(x, y) = \sum z_i b_i(x, y) = z \cdot B(x, y).$$

Choose $b_{e_i}^\dagger(z, y)$ as basis of $B^\dagger$. Identify $B^\dagger$ with the map $B(z, y)^\dagger = \sum_i \bar{e}_i b_i^\dagger(z, y) = \sum_i \bar{e}_i(z \cdot B(e_i, y))$. Finally chose, for defining $B^{\dagger\dagger}$, the isomorphism $e_i \leftrightarrow b_i^\dagger$ and repeat the above process. Then

$$\begin{aligned} B(x, y)^{\dagger\dagger} &= \sum_j \bar{f}_j(x \cdot B^\dagger(f_j, y)) = \sum_j \bar{f}_j(\sum_i (x \cdot \bar{e}_i)(f_j \cdot B(e_i, y))) \\ &= \sum_j \sum_i x_i \bar{f}_j b_j(e_i, y)) = \sum_j \sum_i \bar{f}_j b_j(x_i e_i, y) = B(x, y) \end{aligned}$$

Hence † is a involution. Combinations of † and * can effect an arbitrary permutation of the roles x, y, z and hence lead to 6 subspaces of bilinear forms respectively 6 bilinear maps:

$$B, B^*, B^\dagger, B^{\dagger *}, B^{\dagger *\dagger} = B^{*\dagger *}, B^{*\dagger}$$

We have the following identities:

$$\begin{aligned} z \cdot B(x, y) = z \cdot B^*(y, x) = x \cdot B^\dagger(z, y) = x \cdot B^{\dagger *}(y, z) = y \cdot B^{\dagger *\dagger}(x, z) = y \cdot B^{*\dagger}(z, x) \\ = b_z(x, y) = b_z^*(y, x) = b_x^\dagger(z, y) = b_x^{\dagger *}(y, z) = b_y^{\dagger *\dagger}(x, z) = b_y^{*\dagger}(z, x) \end{aligned} \tag{5}$$

If $n = m$ there is an interpretation of $B^\dagger$ in terms $\mathcal{V}_B$. Chose in the definition of $\mathcal{V}_B^\perp$ the scalar product as $\langle (x, y), (x', y') \rangle := x \cdot y' + x' \cdot y$. Then:

$$\langle (x, B(x, a)), (x', B^\dagger(x', a)) \rangle = x' B(x, a) + x B^\dagger(x, a)$$

By Equation 5 it is $x' B(x, a) = x B^\dagger(x', a)$, hence:

Proposition 7.

$$\mathcal{V}_{B^\dagger} = \mathcal{V}_B^\perp$$

We are now ready to give the defining conditions for dual hyperovals completely in terms of bilinear forms. The following statements are equivalent:

- $\forall z \in \mathbb{F}_2^n : z \cdot B(x, y) = 0$
- $B(x, y) = 0$

Therefore:

$$\begin{array}{rcccccc} \sigma(y) & = & \ker(M_y) & = & \mathsf{rR}(b_y^{*\dagger}(z,x)) & = & \mathsf{lR}(b_y^{\dagger *\dagger}(x,z)) \\ \sigma^{-1}(x) & = & \ker(N_x) & = & \mathsf{rR}(b_x^{\dagger}(z,y)) & = & \mathsf{lR}(b_x^{\dagger *}(y,z)) \end{array}$$

With this observation **B1** and **B3** can be rewritten either in terms of the radicals of bilinear forms or as:

Corollary 3. *$\mathcal{V}_B$ is a dual hyperoval if and only if:*

1. **B4**: *Any $0 \neq b \in B^{*\dagger}$ has rank $m-1$*
   (Equivalently: Any $0 \neq b \in B^{\dagger *\dagger}$ has rank $m-1$)
2. **B5**: *Any $0 \neq b \in B^{\dagger}$ has rank $m-1$.*
   (Equivalently: Any $0 \neq b \in B^{\dagger *}$ has rank $m-1$)

Let $m = n$, f be an APN function and $B_f \subset \mathcal{A}$ the associated alternating bilinear map. We want to see when the dual of the APN-dual hyperoval $\mathcal{V}_{B_f}$, hence (using Proposition 7) $\mathcal{V}_{B_f^{\dagger}}$ is a dual hyperoval.

Use **B4** and **B5** as defining conditions. Hence $\mathcal{V}_{B_f^{\dagger}}$ is a dual hyperoval if and only if every nonzero $b \in B_f^{\dagger\dagger *\dagger}$ has rank $m-1$ and every nonzero $b \in B_f^{\dagger\dagger}$ has rank $m-1$.

As † is an involution and B_f is alternating, so $B_f^{*} = B_f$, this simplifies to: Every nonzero b in $B_f^{\dagger}$ and B_f has to have rank $m-1$.

By assumption f is APN, so by Proposition 6 we have that $\mathcal{V}_{B_f}$ is a dual hyperoval. Hence condition **B5** holds for $\mathcal{V}_{B_f}$. Therefore it only remains to show that every nonzero b in B_f has to have rank $m-1$.

As B_f is alternating all $b \in B_f$ have even rank. This shows that $\mathcal{V}_{B_f^{\dagger}}$ cannot be a dual hyperoval if m is even. If m is odd Corollary 1 implies $\mathcal{V}_{B_f^{\dagger}}$ is a dual hyperoval. Thus we have an alternative proof (relaying essentially on [12, Theorem 5]) of Taniguchi's result [21, Theorem 11]:

Corollary 4. *Let $f : \mathbb{F}_2^m \to \mathbb{F}_2^m$ be an APN function and $B_f(y,x) = f(x+y) + f(x) + f(y) + f(0)$. Then $\mathcal{V}_{B_f^{\dagger}}$ $(= \mathcal{V}_{B_f}^{\perp})$ is a dual hyperoval if and only if m is odd.*

A. Appendix: Details on the trace representation

Any $\mathbf{F}_2$-bilinear function $B(x,y) : \mathbf{F}_{2^m} \times \mathbf{F}_{2^m} \mapsto \mathbf{F}_{2^m}$ can be written as a polynomial in two variables, which is linearized with respect to each of the two variables, so as:

$$B(x,y) = \sum_{i,j=0}^{m-1} a_{i,j} x^{2^i} y^{2^j}, \quad a_{i,j} \in \mathbb{F}_{2^m} \tag{6}$$

Call this a **linearized polynomial in two variables.**

Hence any bilinear function $b(x,y) : \mathbf{F}_{2^m} \times \mathbf{F}_{2^m} \mapsto \mathbf{F}_2$ can be written as the trace of a linearized polynomial in two variables, i.e.

$$b(x,y) = \mathsf{tr}(B(x,y))$$

However this representation of the bilinear function is **not** unique. As $\mathsf{tr}(x) = \mathsf{tr}(x^{2^i})$ we can modify the representation of $b(x,y)$ in the following way.

$$b(x,y) = \mathsf{tr}(\sum_{i,j=0}^{m-1} a_{i,j} x^{2^i} y^{2^j}) = \sum_{i,j=0}^{m-1} \mathsf{tr}(a_{i,j} x^{2^i} y^{2^j}) = \sum_{i,j=0}^{m-1} \mathsf{tr}(a_{i,j}^{2^{-j}} x^{2^{i-j}} y) = \mathsf{tr}(\sum_{i,j=0}^{m-1} a_{i,j}^{2^{-j}} x^{2^{i-j}} y)$$

So we have that

$$b(x,y) = \mathsf{tr}(l(x)y) \text{ with } l(x) = \sum_{k=0}^{m-1} \alpha_k x^{2^k} \text{ where } \alpha_k := \sum_{j=0}^{m-1} a_{k+j,j}^{2^{-j}} \tag{7}$$

The indices are to be understood modulo m. This representation is now unique (the dimension over $\mathbb{F}_2$ of the vector space of bilinear functions is m^2, which is also the dimension over $\mathbb{F}_2$ of the α-tuples in $(\mathbb{F}_{2^m})^m$). This representation is usually dedicated to Delsarte and Goethals [12]. We named this the **trace representation** of a bilinear form.

We also identify $b(x,y)$ with the element $(\alpha_0, \ldots, \alpha_{m-1}) \in (\mathbb{F}_{2^m})^m$ which defines the linearized polynomial l.

The trace representation for alternating bilinear forms

A linearized polynomial $B(x,y)$ in two variables is called **alternating** if $B(x,x) = 0$ (which again implies $B(x,y) = B(y,x)$). In Equation 6 we have therefore $a_{i,i} = 0$ and $a_{i,j} = a_{j,i}$.

Any alternating bilinear form can be written as the trace of an alternating linearized polynomial. This implies for the trace representation of an alternating bilinear form (Equation 7)

$$\alpha_{\cdot\cdot k} = \sum_{j=0}^{m-1} a_{-k+j,j}^{2^{-j}} = \sum_{j=0}^{m-1} a_{j,k+j}^{2^{-j-k}} = (\sum_{j=0}^{m-1} a_{j,k+j}^{2^{-j}})^{2^{-k}} = (\sum_{j=0}^{m-1} a_{k+j,j}^{2^{-j}})^{2^{-k}} = \alpha_k^{2^{-k}}$$

So for alternating forms the following holds:

$$\alpha_0 = 0, \quad \alpha_k = \alpha_{m-k}^{2^k}, \quad \text{Especially if } m = 2r \text{ we have } \alpha_r = \alpha_r^{2^r}, \text{ i.e. } \alpha_r \in \mathbb{F}_{2^r}.$$

So the trace representation of an alternating form is determined by the element

$$(\alpha_1, \ldots \alpha_r) \in \begin{cases} (\mathbb{F}_{2^m})^{r-1} \times \mathbb{F}_{2^{m/2}} & \text{if } m = 2r \\ (\mathbb{F}_{2^m})^r & \text{if } m = 2r+1 \end{cases}$$

A.1. Computing the coefficients of the trace representation

The representations of the a bilinear form, discussed in Section 3, were determined by the m^2 values $m_{i,j} = b(e_i, e_j) \in \mathbb{F}_2$. So these characterizations can be obtained from the trace representation by choosing a basis e_i of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ and calculating $m_{i,j} = b(e_i, e_j) = \mathrm{tr}(l(e_i)e_j)$.

We also want to provide the opposite direction, i.e. to give $l(x)$, more precisely the values α_k, in terms of the $m_{i,j} = b(e_i, e_j) \in \mathbb{F}_2$. This will be done in two steps.

Identify $\mathbb{F}_2^m$ with $\mathbb{F}_{2^m}$ by identifying $x = (x_1, \ldots, x_m) \in \mathbb{F}_2^m$ with $\sum x_i e_i \in \mathbb{F}_{2^m}$.

Step one: We determine the linearized polynomial $l_U(x) = \sum_{i=1}^m \alpha_i X^{2^i}$ effecting the same map as $x \mapsto x^t U$ with some $m \times m$ matrix U, i.e

$$x^t U = \sum_{i,j} x_i u_{i,j} e_j \stackrel{!}{=} \sum_j \alpha_j (\sum_i x_i e_i)^{2^j} = \sum_i x_i \sum_j \alpha_j e_i^{2^j}$$

So we get the α_i as solution of the following $\mathbb{F}_{2^m}$-linear equation:

$$U\mathbf{e} = E\mathbf{a}, \text{ hence } \mathbf{a} = E^{-1}U\mathbf{e}, \text{ with } E_{i,j} = e_i^{2^j}, \quad \mathbf{e} = (e_1, \ldots, e_m)^t, \quad \mathbf{a} = (\alpha_1, \ldots, \alpha_m)^t.$$

Note that E has full rank (see e.g. [13, Bem 2.15.]).

Step two: Let $M = (m_{i,j})$ be the $m \times m$ matrix, defined by $m_{i,j} = b(e_i, e_j) \in \mathbb{F}_2$. Let C be the $m \times m$-matrix over $\mathbb{F}_2$, with $C_{i,j} = tr(e_i, e_j)$. C is the Gram matrix with respect to the basis e_i and the trace form and hence has full rank.

Choosing l as the linearized polynomial $l_{MC^{-1}}$ gives the trace representation of $b(x,y)$. Set

$$x^t MC^{-1} = l(x) =: \sum_i \mathrm{l}_i e_i$$

with this we see that:

$$\mathrm{tr}(l(x)y) = \mathrm{tr}(\sum_{i,j} \mathrm{l}_i e_i y_j e_j) = \sum_{i,j} \mathrm{l}_i C_{i,j} y_j = \mathrm{l}Cy = x^t MC^{-1} Cy = b(x,y)$$

A.2. Dual subspaces in the trace representation

In case that the space of bilinear forms and its dual are denoted in the trace representation we use an adapted scalar product. Let a vector space of bilinear forms B be given by a (generating) set S_B of vectors $(\alpha_1, \ldots, \alpha_m)$ in $(\mathbb{F}_{2^m})^m$. Define the **dual subspace** $B^\perp$ in terms of vectors $S_{B^\perp}$ as

$$S_{B^\perp} := \{(\alpha'_1, \ldots, \alpha'_m) \in (\mathbb{F}_{2^m})^m | \forall (\alpha_1, \ldots, \alpha_m) \in S_B : \mathrm{tr}(\sum_{i=1}^m \alpha_i \alpha'_i) = 0\}$$

And for alternating bilinear forms, where B is given by a (generating) set S_B,

$$S_B \subseteq \begin{cases} (\mathbb{F}_{2^m})^{r-1} \times \mathbb{F}_{2^{m/2}} & \text{if } m = 2r \\ (\mathbb{F}_{2^m})^r & \text{if } m = 2r+1 \end{cases}$$

There are two versions depending on the parity of m.

Case $m = 2r$

$$S_{B^\perp} := \{(\alpha'_1, \ldots, \alpha'_r) \in (\mathbb{F}_{2^m})^{r-1} \times \mathbb{F}_{2^{m/2}} | \forall (\alpha_1, \ldots, \alpha_r) \in S_B : \mathrm{tr}(\sum_{i=1}^{r-1} \alpha_i \alpha'_i) + Tr(\alpha_r \alpha'_r) = 0\}$$

where tr and Tr are the absolute traces in $\mathbb{F}_{2^m}$ respectively $\mathbb{F}_{2^r}$.

Case $m = 2r + 1$

$$S_{B^\perp} := \{(\alpha'_1, \ldots, \alpha'_r) \in (\mathbb{F}_{2^m})^r | \forall (\alpha_1, \ldots, \alpha_r) \in S_B : \mathrm{tr}(\sum_{i=1}^{r} \alpha_i \alpha'_i) = 0\}$$

A.3. Starting from an quadratic (APN) function for m = n

Let $f : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ be a quadratic function with

$$f(x) = x^t A_f x := \sum_{i<j} a_{i,j} x^{2^i + 2^j} + L(x)$$

where $A_f \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ is an upper triangular matrix with main diagonal zero and L is an affine function. The associated bilinear map B_f is the linearized polynomial in two variables $B_f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ with

$$B_f(x, y) := \delta_y f(x) = f(x + y) + f(x) + f(x) + f(0) = x^t (A_f^t + A_f) x = \sum_{i<j} a_{i,j} (x^{2^i} y^{2^j} + x^{2^j} y^{2^i})$$

Identify $B_f(x, y)$ with the m-dimensional vector space of alternating bilinear forms of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \mapsto \mathbb{F}_2$, also called B_f, this vector space consists of the elements

$$\mathrm{tr}(\omega B_f(x, y)) \text{ with } \omega \in \mathbb{F}_{2^m}.$$

Define the currently undefined $a_{i,j}$ with $i \geq j$ by $a_{i,i} = 0$ and $a_{i,j} = a_{j,i}$, so as the coefficients of the matrix by $(A_f^t + A_f)$. Then the linearized polynomial $l_\omega =: \sum_k \alpha_k^{(\omega)} x^{2^k}$ corresponding to $\mathrm{tr}(\omega B_f(x, y))$ has coefficients

$$\alpha_k^{(\omega)} := \sum_{j=0}^{m-1} (\omega a_{k+j,j})^{2^{-j}}$$

Denote the coefficient vector space of B_f as $S_{B_f} := \{(\alpha_1^{(\omega)}, \ldots, \alpha_r^{(\omega)}) | \omega \in \mathbb{F}_{2^m}\}$.

In Section 3.2.2 dual space of $B_f^\perp$ is used. $B_f^\perp$ can be expressed efficiently in terms of f. Choose the scalar product introduced for the trace representation in Section A.2.

Case $m = 2r + 1$

$$S_{B_f^\perp} := \{(\alpha'_1, \ldots, \alpha'_r) \in (\mathbb{F}_{2^m})^r | \forall (\alpha_1, \ldots, \alpha_r) \in S_{B_f} : \mathrm{tr}(\sum_{i=1}^{r} \alpha'_i \alpha_i) = 0\}$$

We modify the trace term:

$$0 = \mathrm{tr}(\sum_{i=1}^{r} \alpha'_i \sum_{j=0}^{m-1} (\omega a_{i+j,j})^{2^{j}}) = \sum_{i=1}^{r} \sum_{j=0}^{m-1} \mathrm{tr}(\alpha'_i (\omega a_{i+j,j})^{2^{j}}) = \sum_{i=1}^{r} \sum_{j=0}^{m-1} \mathrm{tr}(\omega \alpha_i'^{2^j} a_{i+j,j}) = \mathrm{tr}(\omega \sum_{i=1}^{r} \sum_{j=0}^{m-1} \alpha_i'^{2^j} a_{i+j,j})$$

This holds for all $\omega \in \mathbb{F}_{2^m}$, hence is equivalent to $\sum_{i=1}^{r} \sum_{j=0}^{m-1} \alpha_i'^{2^j} a_{i+j,j} = 0$. Define the linearized polynomials λ_i as the linearized polynomial whose coefficients are the i-th diagonal of $(A_f^t + A_f)$, i.e.

$$\lambda_i(x) := \sum_{j=0}^{m-1} a_{i+j,j} x^{2^j}$$

We have shown:

$$S_{B_f^\perp} := \{(\alpha'_1, \ldots, \alpha'_r) \in (\mathbb{F}_{2^m})^r | \sum_{i=1}^{r} \lambda_i(\alpha'_i) = 0\}$$

Case $m = 2r$ Proceed as for odd m. We only have to take special care for the term involving $a_{r+j,j}$. So we already can assume that the condition defining $S_{B_f^\perp}$ is: $\mathrm{tr}(\omega \sum_{i=1}^{r-1} \lambda_i(\alpha'_i)) + Tr(\alpha'_r \sum_{j=0}^{m-1} (\omega a_{r+j,j})^{2^{-j}}) = 0$.

We now transform the Tr Term. Use $a_{i,j} = a_{j,i}$ and $\alpha'_r \in \mathbb{F}_{2^r}$. Let τ be the trace from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^r}$ (i.e. $\tau : x \mapsto x^{2^r} + x$) and observe that $\mathsf{tr} = Tr \circ \tau$.

$$Tr(\alpha'_r \sum_{j=0}^{m-1} (\omega a_{r+j,j})^{2^{-j}}) = Tr(\alpha'_r \sum_{j=0}^{r-1} ((\omega a_{r+j,j})^{2^{-j}} + (\omega a_{r+j+r,j+r})^{2^{-j-r}}))$$

$$= \sum_{j=0}^{r-1} Tr({\alpha'_r}^{2^j} \tau(\omega a_{r+j,j})) = Tr(\tau(\sum_{j=0}^{r-1} {\alpha'_r}^{2^j} \omega a_{r+j,j})) = \mathsf{tr}(\omega \sum_{j=0}^{r-1} {\alpha'_r}^{2^j} a_{r+j,j})$$

Hence our condition for $S_{B_f^\perp}$ is

$$\forall \omega \in \mathbb{F}_{2^m} : 0 = \mathsf{tr}(\omega(\sum_{i=1}^{r} \lambda_i(\alpha'_i) + \sum_{j=0}^{r-1} {\alpha'_r}^{2^j} a_{r+j,j})) \quad \Leftrightarrow \quad 0 = \sum_{i=1}^{r} \lambda_i(\alpha'_i) + \sum_{j=0}^{r-1} {\alpha'_r}^{2^j} a_{r+j,j}$$

Define the linearized[1] polynomial λ_r (over $\mathbb{F}_2^r$) as $\lambda_r(x) := \sum_{j=0}^{r-1} a_{r+j,j} x^{2^j}$. With this we get formally the same condition for $S_{B_f^\perp}$ as in the odd case. We summarize the above results:

Proposition 8. *Let $f(x) = \sum_{i<j} a_{i,j} x^{2^i+2^j} + L(x)$ with alternating map $B_f(x,y) = \sum_{i<j} a_{i,j}(x^{2^i} y^{2^j} + x^{2^j} y^{2^i})$ and $\lambda_i(x) := \sum_{j=0}^{m-1} a_{i+j,j} x^{2^j}$. For $m = 2r+1$ it is*

$$S_{B_f^\perp} := \{(\alpha'_1, \ldots, \alpha'_r) \in (\mathbb{F}_{2^m})^r \mid \sum_{i=1}^{r} \lambda_i(\alpha'_i) = 0\}$$

And for $m = 2r$, with $\lambda_r(x) := \sum_{j=0}^{r-1} a_{r+j,j} x^{2^j}$, it is

$$S_{B_f^\perp} := \{(\alpha'_1, \ldots, \alpha'_r) \in (\mathbb{F}_{2^m})^{r-1} \times \mathbb{F}_{2^r} \mid \sum_{i=1}^{r} \lambda_i(\alpha'_i) = 0\}$$

Observe that f (up to a affine function) , B_f, as well as the λ_i are completely determined by A_f. And that the knowledge of one of f, B_f or $(\lambda_i \mid 1 \le i \le r)$ is sufficient to reconstruct A_f. In particular you can also write f and B in terms of the λ_i:

$$f(x) = \sum_{i=1}^{r} \lambda_i(x^{2^i+1}) \quad \text{and} \quad B_f(x,y) = \sum_{i=1}^{r} ((\lambda_i(x^{2^i} y) + (\lambda_i(x y^{2^i}))$$

A.3.1. Examples

The λ of a monomial: For $f(x) = c x^{(2^i+1)2^j}$, $i < j$, only $\lambda_i(x) = c x^{2^j}$ is nonzero.
So the Gold function $f(x) = x^{2^i+1}$ has as equivalent condition $\alpha'_i = 0$.
The λ of the trace of a monomial: let $i \le (n-1)/2$ and $f(x) = c\,\mathsf{tr}(x^{2^i+1}) = c\,\mathsf{tr}(x^{(2^i+1)2^j}) = c \sum_{l=0}^{m-1} x^{(2^l+1)2^l}$.
Then the only non-zero λ_* is $\lambda_i(x) = \sum_{l=0}^{m-1} x^{2^l} c = c\,\mathsf{tr}(x)$. (For $f(x) = \mathsf{tr}(c x^{2^i+1})$ we get $\lambda_i(x) = \mathsf{tr}(cx)$.)
In the case $m = 2r$, $i = r$ we get the analog result by replacing tr by Tr.

This enables us to give without effort the defining condition for $S_{B_f^\perp}$, if the APN function is given in the form $f = \sum_{i=1}^{\lfloor n/2 \rfloor} g_i$, where g_i is one of the two cases discussed above.
E.g. for the APN function $f(x) = x^3 + \mathsf{tr}(x^9)$ the defining condition is $\alpha'_1 + \mathsf{tr}(\alpha_3) = 0$.

Most of the known quadratic APN have few terms. APN functions for small m can be found in [4, 15, 16]. We provide also a list of the infinite series (as far as currently known to the author).

$f(x) =$	Reference
x^{2^i+1}	$(i,m) = 1$, The Gold function [17]
$x^3 + tr(x^9)$	[7, Corollary 1]
$x^{2^s+1} + w x^{2^{ik}+2^{nk+s}}$	$m = 3k$ further cond. see [6, Corollary 1] and [1]
$x^{2^s+1} + w x^{2^{ik}+2^{nk+s}}$	$m = 4k$ further cond. see [6, Theorem 2] and [1]
$b x^{2^s+1} + b^{2^k} x^{2^{k+s}+2^k} + c x^{2^k+1} + \sum_{i=1}^{k-1} r_i x^{2^{i+k}+2^i}$	$m = 2k$, k, s odd, further cond. see [3, Theorem 1]
$u x^{2^{-k}+2^{k+s}} + u^{2^k} x^{2^s+1} + v x^{2^{k+s}+2^s}$	$m = 3k$, $(s, 3k) = 1$, further cond. see [3, Theorem 3]
$u^{2^k} x^{2^{-k}+2^{k+s}} + u x^{2^s+1} + v x^{2^{-k}+1} + w u^{2^k+1} x^{2^{k+s}+2^s}$	$m = 3k$, $(s, 3k) = 1$, further cond. see [2, Theorem 2.1]
$x^{2^{2i}+2^i} + b x^{2^r+1} + c x^{2^r(2^{2i}+2^i)}$	$m = 2r$, $(i, r) = 1$ further cond. see [5, Corollary 1]
$x(x^{2^i} + x^{2^r} + c x^{2^{i+r}}) + x^{2^i}(c^{2^r} x^{2^r} + s x^{2^{i+r}}) + x^{2^{i+1}2^r}$	$m = 2r$, $(i, r) = 1$ further cond. see [5, Corollary 2]

[1] Note the abuse of notation: $\lambda_r(x) \in \mathbb{F}_{2^m}[x]$ it is $\mathbb{F}_2$-linear only for arguments in $\mathbb{F}_{2^r}$.

References

[1] J. Bierbrauer. A family of crooked functions. *Designs, Codes and Cryptography*, 50:235–241, 2009.

[2] C. Bracken, E. Byrne, N. Markin, and G. McGuire. A few more quadratic APN functions. *http://arxiv.org/pdf/0804.4799*, 2008.

[3] C. Bracken, E. Byrne, N. Markin, and G. McGuire. New families of quadratic almost perfect nonlinear trinomials and multinomials. *Finite Fields And Their Applications*, 14(3):703–714, 2008.

[4] K. A. Browning, J. F. Dillon, R. E. Kibler, and M. T. McQuistan. APN polynomials and related codes. *submitted*, 2008.

[5] L. Budaghyan and C. Carlet. Classes of Quadratic APN trinomials and Hexanomials and Related Structures. *IEEE Transactions on Information Theory*, 54(8):2354–2357, 2008.

[6] L. Budaghyan, C. Carlet, and G. Leander. Two classes of quadratic APN binomials inequivalent to power functions. *IEEE Transactions on Information Theory*, 54(9):4218–4229, 2008.

[7] L. Budaghyan, C. Carlet, and G. Leander. Constructing new APN functions from known ones. *Finite Fields And Their Applications*, 15(2):150–159, 2009.

[8] C. Carlet. *Boolean Methods and Models*, chapter Boolean functions for cryptography and error correcting codes. Cambridge University Press, to appear.

[9] C. Carlet. *Boolean Methods and Models*, chapter Vectorial boolean functions for cryptography. Cambridge University Press, to appear.

[10] R. S. Coulter and M. Henderson. A class of functions and their application in constructing semi-biplanes and association schemes. *Discrete Mathematics*, 202(1):21–32, 1999.

[11] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *Journal of Combinatorial Theory. Series A*, 25(3):226–241, 1978.

[12] P. Delsarte and J. M. Goethals. Alternating bilinear forms over $GF(q)$. *Journal of Combinatorial Theory. Series A*, pages 26–50, 1975.

[13] Y. Edel. *Eine Verallgemeinerung von BCH-Codes*. PhD thesis, Universtität Heidelberg, 1996 (`http://www.mathi.uni-heidelberg.de/~yves/Papers/Diss.html`).

[14] Y. Edel. On quadratic APN functions and dimensional dual hyperovals. *Designs, Codes and Cryptography*, to appear.

[15] Y. Edel, G. Kyureghyan, and A. Pott. A new APN function which is not equivalent to a power mapping. *IEEE Transactions on Information Theory*, 52 (2):744 – 747, 2006.

[16] Y. Edel and A. Pott. A new almost perfect nonlinear function which is not quadratic. *Advances in Mathematics of Communications*, 3(1):59–81, 2009.

[17] R. Gold. Maximal recursive sequences with 3-valued recursive cross-correlation function. *IEEE Transactions on Information Theory*, 14:154–156, 1968.

[18] F. Göloğlu and A. Pott. Almost perfect nonlinear functions: A possible geometric approach. In *Proceedings of the Contact Forum* Coding Theory and Cryptography II *at The Royal Flemish Academy of Belgium for Science and the Arts 2007*, pages 75–100, 2007.

[19] A. Munemasa. An analogue of t-designs in association schemes of alternating bilinear forms. *Graphs and Combinatorics*, 2(1):259–267, 1986.

[20] N. Nakagawa. On the number of generalized quadratic APN functions. Slides for Fq9: `http://mathsci.ucd.ie/~gmg/Fq9Talks/Nakagawa.pdf`.

[21] H. Taniguchi. On the duals of certain d-dimensional dual hyperovals in $PG(2d+1,2)$. *Finite Fields And Their Applications*, 15:673–681, 2009.

[22] S. Yoshiara. Dimensional dual arcs – a survey. In *Finite Geometries, Groups, and Computation: Proceedings of the Conference 'Finite Geometries, Groups, and Computation,' September 4-9, 2004 Pingree Park, Colorado*, 2006.

[23] S. Yoshiara. Dimensional dual hyperovals associated with quadratic APN functions. *Innovations in Incidence Geometry*, (8):147–169, 2008.